Oggetto: Comunicazione riguardo una violazione dei dati personali da parte di Synlab

Gentile Utente,

La informiamo che SYNLAB è stata vittima di un attacco cybercriminale di tipo ransomware, come già reso pubblico dall'azienda stessa e riportato da numerosi mass media nazionali. Questo attacco ha comportato la sottrazione illecita (c.d. esfiltrazione) di una quantità significativa di dati conservati da SYNLAB.

Dettagli della violazione:

A seguito delle verifiche effettuate, SYNLAB ha appurato che tra i dati sottratti vi sono informazioni personali, comprese informazioni anagrafiche e relative allo stato di salute dei pazienti. Questi dati sono trattati da SYNLAB in qualità di Responsabile del Trattamento per conto di LABORATORIO ANALISI S. MARIA S.R.L.

L'organizzazione cybercriminale ha esfiltrato e pubblicato alcuni folder relativi all'applicativo SYNLABNET, contenenti informazioni anagrafiche e sullo stato di salute dei pazienti.

Azioni intraprese:

Appena rilevato la notizia dell'attacco, il team IT di SYNLAB e un team esterno specializzato in cybersecurity hanno adottato:

- misure immediate per ripristinare la sicurezza dell'infrastruttura IT e garantire il graduale ripristino delle attività di SYNLAB;
- informato l'autorità di controllo competente, come richiesto dal GDPR, **Notifica al Garante privacy;**
- condotto una revisione completa dei propri sistemi di sicurezza per prevenire future violazioni.

Possibili rischi e raccomandazioni:

Non è possibile escludere che l'incidente possa portare a tentativi di furto d'identità o altri tentativi di frode. Pertanto, SYNLAB e LABORATORIO ANALISI S. MARIA S.R.L. raccomandano di prestare maggiore attenzione a qualunque interazione sospetta, sia online che offline.

Si invita a consultare le seguenti pagine informative dell'Autorità Garante per la Protezione dei Dati Personali per ulteriori dettagli su come proteggersi:

- Phishing
- Vishing
- Smishing
- Sim Swapping

Misure suggerite:

- Valuti attentamente ogni e-mail, SMS, messaggio o telefonata in cui le vengono richiesti codici di accesso o ulteriori dati personali. Gli istituti bancari e i fornitori di servizi non richiedono mai codici di accesso o password tramite SMS, e-mail o telefonate.

- Valuti attentamente e-mail, SMS e altri messaggi contenenti collegamenti ipertestuali (link) o allegati sospetti: potrebbero essere usati per indirizzarla verso siti web dannosi o farle scaricare software malevoli.
- Sostituisca le password dei propri account (e-mail, social network, forum, ecc.) e, se possibile, attivi l'autenticazione a più fattori. I meccanismi di autenticazione multifattoriale (es. i codici OTP ricevuti dalla banca dopo aver inserito username e password per accedere all'home banking) rafforzano la protezione da accessi indesiderati.
- Informi i propri amici e familiari di essere stato/a vittima di questa violazione, suggerendo loro di prestare attenzione al rischio di ricevere false richieste che sembrano provenire da lei.

Se ha domande o necessita di ulteriori informazioni riguardo questa violazione, non esiti a contattarci attraverso i seguenti canali:

- **Email:** (s.marialaboratorio@gmail.com)
- **Telefono:** (0143 73073)

Ci scusiamo sinceramente per qualsiasi inconveniente causato da questo incidente e la ringraziamo per la sua comprensione e collaborazione.